

# Some bounds of separating hash families

X. Niu and H. Cao \*

Institute of Mathematics,

Nanjing Normal University, Nanjing 210023, China

caohaitao@njnu.edu.cn

## Abstract

Separating hash families were first introduced by Stinson, Trung and Wei. In this paper, we present some new bounds of SHF with small parameter. By the small parameter, we improve previously known bound of types  $\{w, w\}$  and  $\{w_1, w_2\}$ . we also give a construction for strong separating hash family.

**Key words:** Separating hash family, Frameproof code, Strong separating hash family.

## 1 Introduction

Let  $X, Y$  be finite sets of size  $n$  and  $m$ . Let  $\mathcal{F}$  be a family of functions from  $X$  to  $Y$  with  $|\mathcal{F}| = N$ . Given positive integers  $w_1, w_2, \dots, w_t$ , we say that  $\mathcal{F}$  is a  $\{w_1, w_2, \dots, w_t\}$ -separating hash family, denoted by  $\text{SHF}(N; n, m, \{w_1, w_2, \dots, w_t\})$ , if for all pairwise disjoint subsets  $C_1, C_2, \dots, C_t \subseteq X$  with  $|C_i| = w_i$  for  $i = 1, 2, \dots, t$ , there exists some  $f \in \mathcal{F}$  such that  $f(C_i) \cap f(C_j) = \emptyset$  for  $i \neq j$ . So  $f$  is said to separate the sets  $C_1, C_2, \dots, C_t$ . The parameter multiset  $\{w_1, w_2, \dots, w_t\}$  is called the *type* of the separating hash families. For the sake of brevity, we use  $\{w_1^{q_1}, w_2^{q_2}, \dots, w_t^{q_t}\}$  to denote the multiset in which there are exactly  $q_i$  copies of  $w_i$  and  $w_i < w_j$  for  $1 \leq i < j \leq t$ . Further,  $w^1$  will be written as  $w$ .

Separating hash families were first introduced by Stinson, Trung and Wei [32]. It can be used to construct frameproof codes, secure frameproof codes and parent-identifying codes, see [5, 12, 14, 26, 30, 31, 32, 37]. Most results of the known papers on separating hash families are focused on the bounds and constructions, see [4, 6, 7, 10, 18, 19, 22, 23, 33, 36]. Here are some known results related to the main results of this paper.

**Theorem 1.1** ([30]) *If there exists an  $\text{SHF}(N; n, m, \{w, w\})$ , then  $n < m^{\lceil \frac{N}{w} \rceil} + 2w - 2$ .*

**Theorem 1.2** ([7]) *If there exists an  $\text{SHF}(2w; n, m, \{w, w\})$  with  $m \geq 2w \geq 4$ , then  $n < m^2$ .*

---

\*Research supported by the National Natural Science Foundation of China under Grant No. 11571179, the natural science foundation of Jiangsu Province under Grant No. BK20131393, and the Priority Academic Program Development of Jiangsu Higher Education Institution. E-mail: caohaitao@njnu.edu.cn

**Theorem 1.3** ([7]) *If there exists an SHF( $w+1; n, m, \{1, w\}$ ) for each positive integer  $m \geq 1+w$ , then  $n \leq m^2$ .*

**Theorem 1.4** ([7]) *Suppose there exists an SHF( $w_1 + w_2; n, m, \{w_1, w_2\}$ ), where  $m \geq w_1 + w_2$ . Then  $n \leq m^2$ .*

**Theorem 1.5** ([35]) *For positive integers  $q, w_1$  and  $w_2$ , there exists an infinite class of SSHF( $N; n, q, \{w_1, w_2\}$ ) for which  $N$  is  $O((w_1(w_1 + w_2))^{\log^* n} \log n)$ .*

The following Theorem is a known bound for general type  $\{w_1, w_2, \dots, w_t\}$ .

**Theorem 1.6** ([6]) *Let  $t \geq 3$  be an integer. If there exists an SHF( $N; n, m, \{w_1, w_2, \dots, w_t\}$ ), where  $u = \sum_{i=1}^{t-1} w_i$ , then*

$$n < (u-1)(m^{\lceil \frac{N}{u-1} \rceil} - 1) + 1.$$

**Theorem 1.7** ([21]) *Suppose there exists an SHF( $N; n, m, \{w_1, w_2, \dots, w_t\}$ ). Let  $u = \sum_{i=1}^{t-1} w_i$  and let  $1 \leq r \leq u-1$  be the positive integer such that  $N \equiv (\text{mod } u-1)$ . If there exists an SHF( $\lfloor \frac{N}{u-1} \rfloor, n_1, q, \{w_1, w_2, \dots, w_t\}$ ) with  $n_1 \geq u$ , then it holds that  $n \leq r q^{\lceil \frac{N}{u-1} \rceil} + (u-1-r) q^{\lfloor \frac{N}{u-1} \rfloor}$ .*

This paper is organized as blew. In the next section, we give some definitions and prove two lemmas which will be used in Section 3. In Section 3 we give an optimal SHF( $4; 10, 4, \{2, 2\}$ ), and prove two new bounds for an SHF( $4; n, m, \{2, 2\}$ ) and an SHF( $2w; n, m, \{w, w\}$ ) which update the bound in Theorem 1.2. In Section 4 we have an bound of SHF( $2+w; n, m, \{2, w\}$ ), then, by the induction hypothesis, we prove the new bound for an SHF( $w_1 + w_2; n, m, \{w_1, w_2\}$ ) which update the bound in Theorem 1.4. In Section 5 we construct an SSHF by the  $k$ -uniform hypergraph.

## 2 A bound for SHF( $4; n, m, \{2, 2\}$ )

Given an SHF( $N; n, m, \{w_1, w_2, \dots, w_t\}$ ), we often construct an  $N \times n$  matrix  $A = (a_{ij})$  having entries on a set of  $m$  elements such that  $a_{ij} = f_i(x_j)$  where  $f_1, f_2, \dots, f_N$  is some fixed ordering of the functions in  $\mathcal{F}$  and  $x_1, \dots, x_n$  are elements of  $X$ . This matrix is called the *representation matrix* of the SHF.

**Lemma 2.1** ([8]) *If  $A$  is a representation matrix of an SHF( $N; n, m, \{w_1, w_2, \dots, w_t\}$ ), and if  $B$  is a matrix obtained from  $A$  by permuting the rows and/or columns and/or elements, then  $B$  is also a representation matrix of an SHF( $N; n, m, \{w_1, w_2, \dots, w_t\}$ ).*

**Lemma 2.2** *If  $A$  is a representation matrix of an SHF( $4; n, m, \{2, 2\}$ ), then there doesn't exist a submatrix of  $A$  which is isomorphic to  $B$  or  $C$  or  $D$  as below. Such matrixes  $B, C$  and  $D$  are called forbidden matrixes.*

$B$				$C$				$D$			
$a$	$a$	$*$	$*$	$a$	$a$	$*$	$*$	$a$	$a$	$*$	$*$
$b$	$b$	$*$	$*$	$b$	$b$	$*$	$*$	$*$	$b$	$b$	$*$
$*$	$*$	$c$	$c$	$x$	$*$	$x$	$*$	$x$	$*$	$*$	$x$
$*$	$*$	$d$	$d$	$*$	$v$	$*$	$v$	$*$	$*$	$v$	$v$

*Proof:* It is observed that in the matrix  $B$  the sets of columns  $C_1 = \{1, 3\}$  and  $C_2 = \{2, 4\}$  are not separable; in the matrix  $C$  the sets  $C_1 = \{1, 4\}$  and  $C_2 = \{2, 3\}$  are not separable; and in the matrix  $D$  the sets  $C_1 = \{1, 3\}$  and  $C_2 = \{2, 4\}$  are not separable. In all these cases we get a contradiction to the separating property of type  $\{2, 2\}$ .  $\square$

Suppose  $A = (a_{ij})$  is a representation  $N \times n$  matrix of an SHF on  $m$  elements in  $M$ . We need the following notations. Let

$$\lambda_x^i = |\{a_{ij} : a_{ij} = x, 1 \leq j \leq n\}|, \quad 1 \leq i \leq N, \quad x \in M,$$

$$\lambda_{max} = \max\{\lambda_x^i : 1 \leq i \leq N, x \in M\}, \quad \text{and}$$

$$d_{ij}(x, y) = |\{k : a_{ik} = x, a_{jk} = y, 1 \leq k \leq n\}|, \quad 1 \leq i < j \leq N.$$

**Lemma 2.3** *Suppose  $A$  is a representation matrix of an  $\text{SHF}(4; n, m, \{2, 2\})$  with  $m \geq 3$ . If there is a pair of elements  $x$  and  $y$  such that  $d_{ij}(x, y) \geq 2$ , then  $n \leq (m - 1)^2 + 1$ .*

*Proof:* By Lemma 2.1, we may assume  $d_{12}(a, b) \geq 2$ . Then we have a submatrix  $B$  of  $A$  in the following table.

$$B = \begin{array}{|c|c|} \hline a & a \\ \hline b & b \\ \hline x & y \\ \hline u & v \\ \hline \end{array}$$

We distinguish into the following 5 cases.

1.  $\lambda_x^3 = \lambda_y^3 = 1$  or  $\lambda_u^4 = \lambda_v^4 = 1$ . By Lemma 2.1, we only need to consider the former one. Let  $C$  be the  $4 \times (n - 2)$  matrix obtained from  $A$  by removing the matrix  $B$ . Then  $C$  is a representation matrix of an  $\text{SHF}(4; n - 2, m, \{2, 2\})$ , and there are at most  $m - 2$  distinct elements in row three. By the pigeon hole principle, there is an element  $t$  in row four such that  $\lambda_t^4 \geq \lceil \frac{n-2}{m} \rceil$ . By Lemma 2.2 we have  $\lceil \frac{n-2}{m} \rceil \leq m - 2$ . So,  $n \leq m^2 - 2m + 2$ .

2.  $\lambda_x^3 = 1, \lambda_y^3 > 1, \lambda_u^4 = 1, \lambda_v^4 > 1$ . Let  $D$  be the  $4 \times (n - 1)$  matrix obtained from  $A$  by removing column one. Then  $D$  is a representation matrix of an  $\text{SHF}(4; n - 1, m, \{2, 2\})$ , and there are at most  $m - 1$  distinct elements in row three and in row four. By the pigeon hole principle, there is an element  $t$  such that  $\lambda_t^4 \geq \lceil \frac{n-1}{m-1} \rceil$ . By Lemma 2.2 we have  $\lceil \frac{n-1}{m-1} \rceil \leq m - 1$ . So,  $n \leq m^2 - 2m + 2$ .

3.  $\lambda_x^3 = 1, \lambda_y^3 > 1, \lambda_u^4 > 1, \lambda_v^4 = 1$ . By Lemma 2.2 we know that  $\lambda_u^4 = \lambda_y^3 = 2$ , and there exists a submatrix  $E$  of  $A$  as below.

$$E = \begin{array}{|c|c|c|} \hline a & a & * \\ \hline b & b & * \\ \hline x & y & y \\ \hline u & v & u \\ \hline \end{array}$$

Let  $F$  be the  $4 \times (n - 3)$  matrix obtained from  $A$  by removing the matrix  $E$ . Then  $F$  is a representation matrix of an SHF( $4; n - 3, m, \{2, 2\}$ ), and there are  $m - 2$  distinct elements at most in rows three and four. By the pigeon hole principle, there is an element  $t$  such that  $\lambda_t^4 \geq \lceil \frac{n-3}{m-2} \rceil$ . By Lemma 2.2 we have  $\lceil \frac{n-3}{m-2} \rceil \leq m - 2$ . So,  $n \leq m^2 - 4m + 7$ .

4.  $\lambda_x^3 = 1, \lambda_y^3 > 1, \lambda_u^4 > 1, \lambda_v^4 > 1$ . By Lemma 2.2 we know that  $\lambda_u^4 = \lambda_y^3 = 2$ , and there exists a submatrix  $G$  of  $A$  as below.

$$G = \begin{array}{|c|c|c|} \hline a & a & * \\ \hline b & b & * \\ \hline x & y & y \\ \hline u & v & u \\ \hline \end{array}$$

Let  $H$  be the  $4 \times (n - 3)$  matrix obtained from  $A$  by removing the matrix  $G$ . Then  $H$  is a representation matrix of an SHF( $4; n - 3, m, \{2, 2\}$ ), and there are at most  $m - 2$  distinct elements in row three and  $m - 1$  distinct elements in row four. By the pigeon hole principle, there is an element  $t$  such that  $\lambda_t^4 \geq \lceil \frac{n-3}{m-2} \rceil$ . By Lemma 2.2 we have  $\lceil \frac{n-3}{m-2} \rceil \leq m - 1$ . So,  $n \leq m^2 - 3m + 5$ .

5.  $\lambda_x^3 > 1, \lambda_y^3 > 1, \lambda_u^4 > 1, \lambda_v^4 > 1$ . By Lemma 2.2 we know that  $\lambda_x^3 = \lambda_y^3 = \lambda_u^4 = \lambda_v^4 = 2$ , and there exists a submatrix  $M$  of  $A$  as below.

$$M = \begin{array}{|c|c|c|c|} \hline a & a & * & * \\ \hline b & b & * & * \\ \hline x & y & y & x \\ \hline u & v & u & v \\ \hline \end{array}$$

Let  $Q$  be the  $4 \times (n - 3)$  matrix obtained from  $A$  by removing the matrix  $M$ . Then  $Q$  is a representation matrix of an SHF( $4; n - 4, m, \{2, 2\}$ ), and there are at most  $m - 2$  distinct elements in row three and row four respectively. By the pigeon hole principle, there is an element  $t$  such that  $\lambda_t^4 \geq \lceil \frac{n-4}{m-2} \rceil$ . By Lemma 2.2 we have  $\lceil \frac{n-4}{m-2} \rceil \leq m - 2$ . So,  $n \leq m^2 - 4m + 8$ .

Combining the above 5 cases with the condition  $m \geq 3$ , we have obtained  $n \leq (m - 1)^2 + 1$ . The proof is complete.  $\square$

### 3 A bound for SHF( $2w; n, m, \{w, w\}$ )

In this section, we shall give a new bound for an SHF( $2w; n, m, \{w, w\}$ ),  $w \geq 2$ . We also present an optimal SHF( $4; 10, 4, \{2, 2\}$ ).

We start with  $w = 2$ . We will prove that if there exists an  $\text{SHF}(4; n, 4, \{2, 2\})$ , then  $n \leq 10$ . To prove this conclusion, we assume that an  $\text{SHF}(4; 11, 4, \{2, 2\})$  exists and get contradiction.

By Lemma 2.3, it's obvious that  $n \leq 10$  when  $m = 4$  and  $\lambda_{\max} > 4$ . So we only need to consider the case  $\lambda_{\max} \leq 4$ . Then we know that  $3 \leq \lambda_{\max} \leq 4$  since  $4 \times 2 = 8 < 11$ . From now on, in the following lemmas of this section, we always suppose  $A$  is a representation matrix of an  $\text{SHF}(4; 11, 4, \{2, 2\})$ ,  $3 \leq \lambda_{\max} \leq 4$ , and  $d_{ij}(x, y) \leq 1$  for any admissible elements  $x, y$  and parameters  $i, j$ . For convenience, we state these properties in the following lemma.

**Lemma 3.1** *If  $A$  is a representation matrix of an  $\text{SHF}(4; 11, 4, \{2, 2\})$ , then  $3 \leq \lambda_{\max} \leq 4$ ,  $d_{ij}(x, y) \leq 1$  for any admissible elements  $x, y$  and parameters  $i, j$ , and each row of  $A$  is isomorphic to  $R_1$  or  $R_2$  as below.*

$R_1$										$R_2$											
$a$	$a$	$a$	$a$	$b$	$b$	$b$	$*$	$*$	$*$	$*$	$a$	$a$	$a$	$b$	$b$	$b$	$c$	$c$	$c$	$d$	$d$

Next, we will prove four lemmas one by one. Lemma 3.2 will lead to Lemma 3.3. Then we get Lemma 3.4 from Lemma 3.3. At last we obtain Lemma 3.5 by using Lemma 3.4.

**Lemma 3.2** *If  $A$  is a representation matrix of an  $\text{SHF}(4; 11, 4, \{2, 2\})$ , then  $A$  has no two rows both of which are isomorphic to  $R_1$ .*

*Proof:* Assume, by contradiction, that  $A$  has two rows which are both isomorphic to  $R_1$ . Without lose of generality, we assume the first 9 columns of  $A$  is the submatrix as below.

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$
$*$	$*$	$c$	$e$	$e$	$e$	$e$	$c$	$c$
$x$	$y$	$z$	$t$	$x$	$y$	$z$	$*$	$*$
$u$	$v$	$i$	$j$	$a_{45}$	$a_{46}$	$a_{47}$	$*$	$*$

Then by Lemma 3.1 we have  $(a_{45}, a_{46}, a_{47}) = (v, i, u)$  or  $(i, u, v)$ . We distinguish two cases.

1.  $(a_{45}, a_{46}, a_{47}) = (v, i, u)$ . By Lemma 2.2, considering the column sets  $\{3, 4, 5\}$  and  $\{1, 4, 6\}$ , we know that

$$d_{34}(x, i) = d_{34}(z, v) = d_{34}(y, u) = 0. \quad (1)$$

Then  $v \notin \{a_{48}, a_{49}\}$ . Otherwise, without lose of generally, let  $a_{48} = v$ . By Lemma 3.1 we have  $a_{38} = t$ , then we get a submatrix( rows 1, 2, 3, 4 and columns 1, 3, 5, 8 ) which is isomorphic to the forbidden matrix  $D$ . Since  $d_{24}(c, i) = 1$ , then  $(a_{48}, a_{49}) = (j, u)$ .

By Lemma 3.1 and (1), we have  $a_{39} = t$ . Then  $a_{38} = y$ , otherwise  $a_{38} = x$ , we get a forbidden matrix( rows 1, 2, 3, 4 and columns 2, 3, 5, 8 ).

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$*$	$*$	$c$	$e$	$e$	$e$	$e$	$c$	$c$	$*$	$*$
$x$	$y$	$z$	$t$	$x$	$y$	$z$	$y$	$t$	$*$	$*$
$u$	$v$	$i$	$j$	$v$	$i$	$u$	$j$	$u$	$*$	$*$

By Lemma 2.2, considering the column sets  $\{1, 3, 8\}$  and  $\{2, 3, 9\}$ , we have  $d_{34}(x, j) = d_{34}(t, v) = 0$ . Thus, by Lemma 3.1 and (1), we have  $d_{34}(z, j) = d_{34}(t, i) = 1$ . So we have determined all these elements of the last two rows.

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$*$	$*$	$c$	$e$	$e$	$e$	$e$	$c$	$c$	$*$	$*$
$x$	$y$	$z$	$t$	$x$	$y$	$z$	$y$	$t$	$z$	$t$
$u$	$v$	$i$	$j$	$v$	$i$	$u$	$j$	$u$	$j$	$i$

By Lemma 3.1, there exists an element  $f \in \{a_{21}, a_{22}\}$  such that  $\lambda_f^2 \geq 2$ . Suppose  $a_{2l} = a_{2k} = f$ ,  $l \in \{1, 2\}$ ,  $k \in \{10, 11\}$ . By Lemma 2.2, considering the column set  $\{1, 2, k\}$ , we have  $d_{34}(a_{3m}, a_{4k}) = d_{34}(a_{3k}, a_{4m}) = 0$ ,  $m = \{1, 2\} \setminus \{l\}$ . This always gives a contradiction.

2.  $(a_{45}, a_{46}, a_{47}) = (i, u, v)$ . By Lemma 2.2, considering the column sets  $\{1, 4, 7\}$  and  $\{2, 4, 5\}$ , we know that

$$d_{34}(x, v) = d_{34}(z, u) = d_{34}(y, i) = 0. \quad (2)$$

Then  $u \notin \{a_{48}, a_{49}\}$ . Otherwise, without loss of generality, let  $a_{48} = u$ . By Lemma 3.1 we have  $a_{38} = t$ , then we get a submatrix( rows 1, 2, 3, 4 and columns 2, 3, 6, 8 ) which is isomorphic to the forbidden matrix  $D$ . Since  $d_{24}(c, i) = 1$ , then  $(a_{48}, a_{49}) = (j, v)$ .

By Lemma 3.1 and (2), we have  $a_{39} = t$ . Then  $a_{38} = x$ , otherwise  $a_{38} = y$ , we get a forbidden matrix( rows 1, 2, 3, 4 and columns 1, 3, 6, 8 ).

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$*$	$*$	$c$	$e$	$e$	$e$	$e$	$c$	$c$	$*$	$*$
$x$	$y$	$z$	$t$	$x$	$y$	$z$	$x$	$t$	$*$	$*$
$u$	$v$	$i$	$j$	$i$	$u$	$v$	$j$	$v$	$*$	$*$

By Lemma 2.2, considering the column sets  $\{2, 3, 8\}$  and  $\{1, 3, 9\}$ , we have  $d_{34}(y, j) = d_{34}(t, u) = 0$ . Thus, by Lemma 3.1 and (2), we have  $d_{34}(z, j) = d_{34}(t, i) = 1$ . So we have determined all these elements of the last two rows.

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$*$	$*$	$c$	$e$	$e$	$e$	$e$	$c$	$c$	$*$	$*$
$x$	$y$	$z$	$t$	$x$	$y$	$z$	$x$	$t$	$z$	$t$
$u$	$v$	$i$	$j$	$i$	$u$	$v$	$j$	$v$	$j$	$i$

By Lemma 3.1, there exists an element  $f \in \{a_{21}, a_{22}\}$  such that  $\lambda_f^2 \geq 2$ . Suppose  $a_{2l} = a_{2k} = f$ ,  $l \in \{1, 2\}$ ,  $k \in \{10, 11\}$ . By Lemma 2.2, considering the column set  $\{1, 2, k\}$ , we have  $d_{34}(a_{3m}, a_{4k}) = d_{34}(a_{3k}, a_{4m}) = 0$ ,  $m = \{1, 2\} \setminus \{l\}$ . This always gives a contradiction.  $\square$

**Lemma 3.3** *If  $A$  is a representation matrix of an  $SHF(4; 11, 4, \{2, 2\})$ , then none row of matrix  $A$  is isomorphic to  $R_1$ .*

*Proof:* By Lemma 3.2, we know that  $A$  has no two rows which are both isomorphic to  $R_1$ . So we assume that the first row of  $A$  is isomorphic to  $R_1$  and the other of  $A$  are isomorphic to  $R_2$ . Without loss of generality, we start with the following submatrix.

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$b$	$c$	$d$	$e$	$b$	$b$	$c$	$c$	$d$	$d$	$e$
$x$	$y$	$z$	$t$	$*$	$*$	$*$	$*$	$*$	$*$	$x$
$u$	$v$	$i$	$j$	$*$	$*$	$*$	$*$	$*$	$*$	$*$

By Lemma 3.1,  $a_{4,11} = v$  or  $i$ . By Lemma 2.1, we only consider  $a_{4,11} = v$ . By Lemma 2.2, considering the column set  $\{3, 4, 11\}$ , we have

$$d_{34}(z, v) = d_{34}(x, i) = 0. \quad (3)$$

1.  $\lambda_x^3 = 2$ . Then  $\lambda_y^3 = \lambda_z^3 = \lambda_t^3 = 3$ . By Lemma 3.1 we can get the following matrix.

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$b$	$c$	$d$	$e$	$b$	$b$	$c$	$c$	$d$	$d$	$e$
$x$	$y$	$z$	$t$	$z$	$y$	$z$	$t$	$y$	$t$	$x$
$u$	$v$	$i$	$j$	$*$	$*$	$*$	$*$	$*$	$*$	$v$

Since  $d_{24}(b, u) = d_{34} = 1$  and (3), we have  $a_{45} = j$ , then  $a_{47} = u$ . So we have a submatrix (rows 1, 2, 3, 4 and columns 2, 4, 5, 7) which is isomorphic to forbidden matrix  $D$ , a contradiction.

2.  $\lambda_x^3 = 3$ .

(i)  $d_{23}(c, x) = 1$ , let  $a_{37} = x$ . Since  $d_{34}(x, u) = d_{34}(x, v) = 1$ , we have  $a_{47} = j$  by (3). By Lemma 2.2, considering the column set  $\{2, 3, 7\}$  we have  $d_{34}(z, j) = 0$ . Then  $\lambda_z^3 = 2$  and  $d_{34}(z, u) = 1$  by (3). Since  $d_{24}(b, u) = d_{23}(d, z) = 1$ , we get  $(a_{38}, a_{48}) = (z, u)$ .

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$b$	$c$	$d$	$e$	$b$	$b$	$c$	$c$	$d$	$d$	$e$
$x$	$y$	$z$	$t$	$*$	$*$	$x$	$z$	$*$	$*$	$x$
$u$	$v$	$i$	$j$	$*$	$*$	$j$	$u$	$*$	$*$	$v$

Thus, the column sets  $C_1 = \{2, 7\}$  and  $C_2 = \{4, 8\}$  are not separable, a contradiction.

- (ii)  $d_{23}(c, x) = 0$ , let  $a_{39} = x$ . Since  $d_{34}(x, u) = d_{34}(x, v) = 1$ , so  $a_{49} = j$  by (3).

$a$	$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$b$	$c$	$d$	$e$	$b$	$b$	$c$	$c$	$d$	$d$	$e$
$x$	$y$	$z$	$t$	$*$	$*$	$*$	$*$	$x$	$*$	$x$
$u$	$v$	$i$	$j$	$*$	$*$	$*$	$*$	$j$	$*$	$v$

Thus, the column sets  $C_1 = \{2, 9\}$  and  $C_2 = \{3, 11\}$  are not separable, a contradiction.  $\square$

**Lemma 3.4** *If  $A$  is a representation matrix of an  $\text{SHF}(4; 11, 4, \{2, 2\})$  and each row of  $A$  is isomorphic to  $R_2$ , then there exists a submatrix  $B$  satisfying  $\lambda_e^2 = \lambda_f^2 = \lambda_g^2 = 3$  and  $\lambda_x^3 = \lambda_y^3 = \lambda_z^3 = 3$ .*

$$B = \begin{array}{|c|c|c|} \hline a & a & a \\ \hline e & f & g \\ \hline x & y & z \\ \hline \end{array}$$

*Proof:* Suppose that the  $A$  does not contains a submatrix which is isomorphic to  $B$ , then we only show that  $A$  is not a representation matrix of an  $\text{SHF}(4; 11, 4, \{2, 2\})$ . Since each row of  $A$  is isomorphic to  $R_2$ , let  $\lambda_d^1 = \lambda_h^2 = \lambda_t^3 = \lambda_j^4 = 2$ . By Lemma 2.1, we have the following submatrix, where I, II and III are  $3 \times 3$  matrixs, and IV is a  $3 \times 2$  matrix.

$a$	$a$	$a$	$b$	$b$	$b$	$c$	$c$	$c$	$d$	$d$
I			II			III			IV	

If there are at most one elements  $x$  in  $\{h, t, j\}$  satisfying  $d_{1k}(a, x) = 1$ , then the first three columns removing the  $i - th$  row form a submatrix which is isomorphic to  $B$ . So the matrix I contain at least two elements in  $\{h, t, j\}$ . Similarly, the matrixs II and III also contain at least two elements in  $\{h, t, j\}$ . Since  $\lambda_h^2 = \lambda_t^3 = \lambda_j^4 = 2$ , we have each of matrixs of I, II and III containg two elements of  $\{h, t, j\}$ . So the matrix IV contain not any one element of  $\{h, t, j\}$ . Thus, for any two elements  $x, y$  in  $\{d, h, t, j\}$ ,  $d_{k_1 k_2}(x, y) = 0$ ,  $\{k_1, k_2\} \subset \{1, 2, 3, 4\}$ . By Lemma 2.1, we have the following submatrix.

$d$	$d$							$a$	$b$	$b$
		$h$	$h$					$e$	$f$	$h$
$x$	$y$	$x$	$z$	$t$	$t$			$x$	$y$	$z$
$v$		$i$				$j$	$j$	$u$	$v$	$i$

Since  $a_{42}$  and  $a_{44}$  in the set  $\{u, v, i\}$ , we have  $(a_{42}, a_{44}) = (u, u)$  or  $(a_{42}, a_{44}) = (i, u)$  or  $(a_{42}, a_{44}) = (u, v)$ . If  $(a_{42}, a_{44}) = (u, u)$ , then the column sets  $C_1 = \{1, 4\}$  and  $C_2 = \{2, 3\}$  are not separable, a contradiction; If  $(a_{42}, a_{44}) = (i, u)$ , then  $(a_{13}, a_{14}) = (b, b)$  by Lemma 3.1, a contradiction; If  $(a_{42}, a_{44}) = (u, v)$ , then  $(a_{13}, a_{14}) = (g, g)$  by Lemma 3.1, a contradiction.  $\square$

**Lemma 3.5** *If  $A$  is a representation matrix of an  $\text{SHF}(4; 11, 4, \{2, 2\})$ , then there is at least one row of  $A$  is isomorphic to  $R_1$ .*

*Proof:* Assume that every row of  $A$  is isomorphic to  $R_2$ . By Lemma 3.4, we suppose the first three rows and columns is a submatrix which is isomorphic to  $B$  satisfying  $\lambda_e^2 = \lambda_f^2 = \lambda_g^2 = 3$  and  $\lambda_x^3 = \lambda_y^3 = \lambda_z^3 = 3$ . Suppose the fourth elements in rows two and three are  $h$  and  $t$  respectively. Then  $\lambda_h^2 = \lambda_t^3 = 2$ . We distinguish two cases.

1.  $d_{23}(h, t) = 0$ . Without lose of generality, let  $d_{23}(e, t) = d_{23}(f, t) = 1$ .
  - (i)  $a_{35} = a_{37}$ . Since  $d_{23}(e, x) = d_{23}(f, y) = 1$ , we have  $a_{35} = a_{37} = z$ .



$a$	$a$	$a$	*	*	*	*	*	*	*	*
$e$	$f$	$g$	$e$	$e$	$f$	$f$	$g$	$g$	$h$	$h$
$x$	$y$	$z$	$t$	$z$	$t$	$z$	$x$	$y$	$x$	$y$
$u$	$v$	$i$	*	*	*	*	*	*	*	*

By Lemma 2.2, the possible elements of each position in the last row are listed as below.

$a_{4k}$	$a_{44}$	$a_{45}$	$a_{46}$	$a_{47}$	$a_{48}$	$a_{49}$	$a_{4,10}$	$a_{4,11}$
possible elements	$v, j$	$v, j$	$u, j$	$u, j$	$v, j$	$u, j$	$i, j$	$i, j$

So we know that  $\lambda_i^4 = 2$  and  $\lambda_u^4 = \lambda_v^4 = \lambda_j^4 = 3$ .

If  $a_{44} = v$ , by Lemma 3.1, we have  $a_{45} = j$ , then  $a_{47} = u$ . So  $a_{46} = j$ . By Lemma 2.2, considering the column sets  $\{1, 2, 5\}$  and  $\{1, 2, 6\}$ , we have  $d_{34}(y, j) = d_{34}(x, j) = 0$ , then  $a_{4,10} = a_{4,11} = i$ , so  $d_{24}(h, i) = 2$ , a contradiction;

If  $a_{44} = j$ , by Lemma 3.1, we have  $a_{45} = v$  and  $a_{46} = u$ , then  $a_{47} = j$ . By Lemma 2.2, considering the column sets  $\{1, 2, 4\}$  and  $\{1, 2, 7\}$ , we have  $d_{34}(y, j) = d_{34}(x, j) = 0$ , then  $a_{4,10} = a_{4,11} = i$ , so  $d_{24}(h, i) = 2$ , a contradiction.

(ii)  $a_{35} \neq a_{37}$ . We distinguish three cases,  $(a_{35}, a_{37}) = (y, x)$ ,  $(a_{35}, a_{37}) = (y, z)$  and  $(a_{35}, a_{37}) = (z, x)$ . If  $(a_{35}, a_{37}) = (y, x)$ , then  $(a_{3,10}, a_{3,11}) = (z, z)$ , a contradiction.  $(a_{35}, a_{37}) = (y, z)$  and  $(a_{35}, a_{37}) = (z, x)$  are isomorphic. So let  $(a_{35}, a_{37}) = (z, x)$ .

$a$	$a$	$a$	*	*	*	*	*	*	*	*
$e$	$f$	$g$	$e$	$e$	$f$	$f$	$g$	$g$	$h$	$h$
$x$	$y$	$z$	$t$	$z$	$t$	$x$	$x$	$y$	$y$	$z$
$u$	$v$	$i$	*	*	*	*	*	*	*	*

Similarly, we have the following table.

$a_{4k}$	$a_{44}$	$a_{45}$	$a_{46}$	$a_{47}$	$a_{48}$	$a_{49}$	$a_{4,10}$	$a_{4,11}$
possible elements	$v, j$	$v, j$	$u, j$	$i, j$	$v, j$	$u, j$	$i, j$	$u, j$

If  $a_{44} = v$ , by Lemma 3.1, we have  $a_{45} = j$  and  $a_{4,11} = u$ . By Lemma 2.2, considering the column set  $\{1, 2, 5\}$ , we have  $d_{34}(y, j) = 0$ , then  $a_{49} = u$  and  $a_{4,10} = j$ . So  $a_{45} = j$ . By Lemma 2.2, considering the column set  $\{2, 3, 6\}$ , we have  $d_{34}(z, j) = 0$ , a contradiction.

If  $a_{44} = j$ , by Lemma 3.1 we have  $a_{45} = v$ , then  $a_{46} = u$ . By Lemma 2.2, considering the column sets  $\{1, 2, 4\}$  and  $\{1, 3, 4\}$ , we have  $d_{34}(y, j) = d_{34}(z, j) = 0$ , so  $a_{49} = a_{4,11} = u$ . Thus,  $\lambda_u^4 = 4$ , a contradiction.

2.  $d_{23}(h, t) = 1$ . Without loss of generality, let  $d_{23}(g, t) = 1$ .

$a$	$a$	$a$	*	*	*	*	*	*	*	*
$e$	$f$	$g$	$e$	$e$	$f$	$f$	$g$	$g$	$h$	$h$
$x$	$y$	$z$	$y$	$z$	$x$	$z$	$x$	$t$	$t$	$y$
$u$	$v$	$i$	*	*	*	*	*	*	*	*

Similarly, we have the following table.

$a_{4k}$	$a_{44}$	$a_{45}$	$a_{46}$	$a_{47}$	$a_{48}$	$a_{49}$	$a_{4,10}$	$a_{4,11}$
element	$i, j$	$v, j$	$i, j$	$u, j$	$v, j$	$u, v, j$	$i, j$	$u, j$

(i)  $\lambda_u^4 = 2$ .

If  $a_{49} = u$  or  $a_{4,11} = u$ , then we have a submatrix(rows 2,3,4 and columns 3,5,7 or 2,6,7 ) which is isomorphic to matrix  $B$  in Lemma 3.4. So by the case 1, we have a contradiction;

If  $a_{47} = u$ , by Lemma 3.1, we have  $a_{4,11} = j$ , then  $a_{44} = a_{4,10} = i$ . If  $a_{45} = j$  or  $a_{48} = j$ , then considering the column sets  $\{1, 2, 5\}$  or  $\{2, 3, 8\}$ , we have  $d_{34}(y, j) = 0$  contradict with  $d_{34}(y, j) = 1$ . So  $a_{45} = a_{48} = v$ . Thus,  $a_{46} = a_{49} = j$ . By Lemma 2.2, considering the column set  $\{1, 3, 9\}$ , we have  $d_{34}(x, j) = 0$ , a contradiction.

$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$e$	$f$	$g$	$e$	$e$	$f$	$f$	$g$	$g$	$h$	$h$
$x$	$y$	$z$	$y$	$z$	$x$	$z$	$x$	$t$	$t$	$y$
$u$	$v$	$i$	$i$	$v$	$j$	$u$	$v$	$j$	$i$	$j$

(ii)  $\lambda_v^4 = 2$ .

If  $a_{45} = v$  or  $a_{48} = v$  or  $a_{49} = v$ , then we have a submatrix(rows 2,3,4 and columns 1,6,8 or 1,4,5 or 1,6,8 ) which is isomorphic to matrix  $B$  in Lemma 3.4. By the case 1, we have a contradiction;

(iii)  $\lambda_i^4 = 2$ .

If  $a_{44} = i$  or  $a_{48} = v$ , then we have a submatrix(rows 2,3,4 and columns 1,6,8 or 1,4,5 ) which is isomorphic to matrix  $B$  in Lemma 3.4. By the case 1, we have a contradiction;

If  $a_{4,10} = i$ , then  $a_{44} = a_{46} = j$ . By Lemma 2.2, considering the column set  $\{1, 3, 4\}$ , we have  $d_{34}(z, j) = 0$ , then  $a_{49} = j$ . Considering the column set  $\{1, 2, 9\}$ , we have  $d_{34}(x, j) = 0$ , a contradiction.

$a$	$a$	$a$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$e$	$f$	$g$	$e$	$e$	$f$	$f$	$g$	$g$	$h$	$h$
$x$	$y$	$z$	$y$	$z$	$x$	$z$	$x$	$t$	$t$	$y$
$u$	$v$	$i$	$j$	$*$	$j$	$*$	$*$	$j$	$i$	$*$

(iv)  $\lambda_j^4 = 2$ .

(a)  $a_{49} = u$ . By Lemma 2.2, considering the column set  $\{2, 3, 9\}$ , we have  $d_{34}(y, u) = 0$ , then  $a_{4,11} = j$ . Thus,  $a_{44} = a_{4,10} = i$ . Since  $\lambda_i^4 = 3$ , so  $a_{46} = j$ . then we have a submatrix(rows 2, 3, 4 and columns 3, 5, 7 ) which is isomorphic to matrix  $B$  in Lemma 3.4. By the case 1, we have a contradiction;

(b)  $a_{49} = v$ . By Lemma 3.1,  $a_{47} = a_{4,11} = u$ . By Lemma 2.2, considering the column set  $\{1, 3, 9\}$ , we have  $d_{34}(x, v) = 0$ , then  $a_{48} = j$  and  $a_{46} = i$ . Considering the column set  $\{2, 3, 8\}$ , we have  $d_{34}(y, j) = 0$ , then  $a_{44} = i$ . So  $a_{4,10} = j$ .

$a$	$a$	$a$	$b$	$c$	$*$	$*$	$*$	$*$	$*$	$*$
$e$	$f$	$g$	$e$	$e$	$f$	$f$	$g$	$g$	$h$	$h$
$x$	$y$	$z$	$y$	$z$	$x$	$z$	$x$	$t$	$t$	$y$
$u$	$v$	$i$	$i$	$v$	$i$	$u$	$j$	$v$	$j$	$u$

Since the first row is isomorphic to  $R_2$ , we have  $\lambda_b^1 = 3$  or  $\lambda_c^1 = 3$ . Then  $a_{16} \neq b$  and  $a_{1,11} \neq b$  by Lemma 3.1. Further, by Lemma 2.2,  $a_{18} \neq b$ ,  $a_{19} \neq b$  and  $a_{1,10} \neq b$ . So we have  $a_{17} = b$ . Thus,  $\lambda_b^1 = 2$  and  $\lambda_c^1 = 3$ . By Lemma 3.1,  $a_{18} \neq c$  and  $a_{1,10} \neq c$ . By Lemma 2.2,  $a_{19} \neq c$ . Then  $a_{16} = a_{1,10} = c$ . Thus  $a_{18} = a_{19} = d$  contradict with Lemma 3.1.

$a$	$a$	$a$	$b$	$c$	$c$	$b$	$*$	$*$	$*$	$*$
$e$	$f$	$g$	$e$	$e$	$f$	$f$	$g$	$g$	$h$	$h$
$x$	$y$	$z$	$y$	$z$	$x$	$z$	$x$	$t$	$t$	$y$
$u$	$v$	$i$	$i$	$v$	$i$	$u$	$j$	$v$	$j$	$u$

(c)  $a_{49} = j$ . By Lemma 3.1,  $a_{47} = a_{4,11} = u$  and  $a_{45} = a_{48} = v$ . By Lemma 2.2, considering the column sets  $\{1, 3, 9\}$  and  $\{2, 3, 9\}$ , we have  $d_{34}(x, j) = d_{34}(y, j) = 0$ . Since  $d_{34}(z, i) = d_{34}(z, v) = d_{34}(z, u) = 1$ , we have  $d_{34}(z, j) = 0$ . Thus  $\lambda_j^4 = 1$ , a contradiction.  $\square$

It's obvious that Lemmas 3.5 is contradicting with Lemma 3.3. So we have the following lemma.

**Lemma 3.6** *If there is an  $SHF(4; n, 4, \{2, 2\})$ , then  $n \leq 10$ .*

**Example 3.7** *There exists an  $SHF(4; 10, 4, \{2, 2\})$ .*

1	1	1	2	2	2	3	3	3	4
1	2	3	1	2	3	1	2	3	4
1	2	3	2	3	1	3	1	2	4
1	2	3	3	1	2	2	3	1	4

**Theorem 3.8** *There exists an optimal  $SHF(4; 10, 4, \{2, 2\})$ .*

*Proof:* The conclusion comes from Lemma 3.6 and Example 3.7.  $\square$

**Theorem 3.9** *If there exists an  $SHF(4; n, m, \{2, 2\})$  with  $m \geq 4$ , then  $n \leq m^2 - m$ .*

*Proof:* If  $m = 4$ , the conclusion follows by Lemma 3.6. If  $m > 4$ , let  $A$  be a representation matrix of an  $SHF(4; n, m, \{2, 2\})$ . Now, we consider the following two cases.

1. There is a pair of elements  $x$  and  $y$  in the  $i$ -th row and the  $j$ -th row respectively such that  $d_{ij}(x, y) > 1$ . Then we have  $n \leq (m-1)^2 + 1 < m^2 - m$  by Lemma 2.3.

2.  $d_{ij}(x, y) \leq 1$  for any admissible elements  $x, y$  and parameters  $i, j$ . Then we have  $\lambda_{max} \leq m$ . Assume, for a contradiction that  $n = m^2 - m + 1$ . By the pigeon hole principle, there is an element  $t_i$  such that  $\lambda_{t_i}^i \geq \lceil \frac{n}{m} \rceil = m$  for  $1 \leq i \leq 4$ . So we have  $\lambda_{max} = m$ .

If there are two elements  $a$  and  $k$  in different rows (without lose of generality, in the first two rows) such that  $\lambda_a^1 = \lambda_k^2 = m$ . Then there is a submatrix of  $A$  as blew.

$a$	$a$	$\cdots$	$a$	$a$	$*$	$*$	$\cdots$	$*$
$*$	$*$	$\cdots$	$*$	$k$	$k$	$k$	$\cdots$	$k$
$x_1$	$x_2$	$\cdots$	$x_{m-1}$	$x_m$	$y_1$	$y_2$	$\cdots$	$y_{m-1}$
$u_1$	$u_2$	$\cdots$	$u_{m-1}$	$u_m$	$v_1$	$v_2$	$\cdots$	$v_{m-1}$

By Lemma 2.2,  $d_{34}(x_i, v_j) = 0$  and  $d_{43}(u_i, y_j) = 0$  for any  $u_i \neq v_j, x_i \neq y_j, 1 \leq i, j \leq m-1$ . So, there are at least  $(m-1) \times (m-3)$  distinct pairs of elements  $s$  and  $t$  such that  $d_{34}(s, t) = 0$ . Thus,  $(m-1) \times (m-3) + n \leq m^2$ , ie.  $m \leq 4$ , then it contradicts with  $m > 4$ ;

Otherwise, there is exactly one row (without lose of generality, the first row) containing an element  $a$  such that  $\lambda_a^1 = m$ .

$a$	$a$	$\cdots$	$a$	$a$	$*$	$*$	$\cdots$	$*$
$*$	$*$	$\cdots$	$*$	$k$	$k$	$k$	$\cdots$	$k$
$x_1$	$x_2$	$\cdots$	$x_{m-1}$	$x_m$	$y_1$	$y_2$	$\cdots$	$x_{m-2}$
$u_1$	$u_2$	$\cdots$	$u_{m-1}$	$u_m$	$v_1$	$v_2$	$\cdots$	$v_{m-2}$

Similarly, we can obtain  $(m-2) \times (m-3)$  distinct pairs of elements  $s$  and  $t$  such that  $d_{34}(s, t) = 0$ . Since  $\lambda_{x_m}^3 \leq m-1$  and  $\lambda_{u_m}^4 \leq m-1$ , we know that there are two elements  $w$  in row three and  $z$  in row four such that  $d_{34}(x_m, z) = d_{34}(w, u_m) = 0$ . Thus,  $(m-2) \times (m-3) + 2 + n \leq m^2$ , ie.  $m \leq 4$ , then it contradicts with  $m > 4$ .  $\square$

Now we are in the position to prove the main result of this section.

**Theorem 3.10** *If there exists an SHF( $2w; n, m, \{w, w\}$ ) with  $m \geq 2w \geq 4$ , then  $n \leq m^2 - m$ .*

*Proof:* We use induction on  $w$  to prove the theorem.

1. By Theorem 3.9, for  $w = 2$  this theorem satisfies.
2. Assume  $w \geq 3$  and there does not exist an SHF( $2w-2; m^2-m, m, \{w-1, w-1\}$ ). Now, we need to prove that there does not exist an SHF( $2w; m^2-m, m, \{w, w\}$ ).

Suppose that there is an SHF( $2w; m^2-m, m, \{w, w\}$ ). Let  $A$  be a representation matrix of an SHF( $2w; m^2-m, m, \{w, w\}$ ), and  $\mathcal{C}$  denote the set of columns of  $A$ . By removing the first two rows of  $A$ , we obtain a  $(2w-2) \times (m^2-m)$  submatrix  $B$ . By inductive hypothesis, there are two sets of columns  $C_1$  and  $C_2$  in  $B$  with  $|C_1| = |C_2| = w-1$  which are not separable. Now, we consider the same column sets  $C_1$  and  $C_2$  in  $A$ . Let  $D = \mathcal{C} \setminus (C_1 \cup C_2)$ , then  $|D| \geq m^2 - 2m + 2$ . If  $C_1$  and  $C_2$  are not separable in the first two rows, then we have  $C_1$  and  $C_2$  are not separable in  $A$ , a contraction; If  $C_1$  and  $C_2$  are not separable in the first row or the second row, then there exist two different columns  $c_1$  and  $c_2$  in  $D$  such that  $a_{2,c_1} = a_{2,c_2}$  or  $a_{1,c_1} = a_{1,c_2}$ . Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ , a contraction. Now, we consider the  $C_1$  and  $C_2$  are separable in the first two rows.

Let  $X_i$  ( $i = 1, 2$ ) be the element set in which each element appears in the  $i$ -th row of these columns in  $D$ . Suppose that  $|X_1| \geq |X_2|$ . Now we distinguish into the following 4 cases.

(i)  $|X_1| \leq m - 2$ . Since  $\frac{n-2(w-1)}{m-2} > m$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ .

(ii)  $|X_1| = |X_2| = m - 1$ . Since  $\frac{n-2(w-1)}{m-1} > m - 1$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ .

(iii)  $|X_1| = m$  and  $|X_2| = m - 1$ . For any column  $k_i \in C_i$  ( $i = 1, 2$ ), we have  $a_{1,k_1} \in X_1$ ,  $a_{1,k_2} \in X_1$ , and  $\{a_{2,k_1}, a_{2,k_2}\} \cap X_2 \neq \emptyset$ . Without loss of generality, let  $a_{2,k_1} \in X_2$ . If there exist two columns  $l_1$  and  $l_2$  in  $D$ , such that  $a_{1,k_2} = a_{1,l_1}$  and  $a_{2,k_1} = a_{2,l_2}$ , we have that  $C_1 \cup \{l_2\}$  is not separated from  $C_2 \cup \{l_1\}$ ; Otherwise, there is a unique column  $l$  such that  $a_{1,k_2} = a_{1,l}$ , and  $a_{2,k_1} = a_{2,l}$ . We remove this column  $l$  from  $D$ , then there are  $m - 1$  distinct elements in the first row of column set  $D \setminus \{l\}$  and  $m - 2$  distinct elements in the second row of column set  $D \setminus \{l\}$ . Since  $\frac{n-2(w-1)-1}{m-1} > m - 2$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D \setminus \{l\}$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ .

(iv)  $|X_1| = |X_2| = m$ . For any column  $k_i \in C_i$  ( $i = 1, 2$ ), we have  $a_{1,k_1} \in X_1$ ,  $a_{1,k_2} \in X_1$ ,  $a_{2,k_1} \in X_2$  and  $a_{2,k_2} \in X_2$ . If there exist distinct columns  $l_1$  and  $l_2$  in  $D$ , such that  $a_{1,k_2} = a_{1,l_1}$  and  $a_{2,k_1} = a_{2,l_2}$ , we have that  $C_1 \cup \{l_1\}$  is not separated from  $C_2 \cup \{l_2\}$ . Otherwise, there only exists a column  $l$  such that  $a_{1,k_2} = a_{1,l}$ , and  $a_{2,k_1} = a_{2,l}$ .

If there exist distinct columns  $l_3$  and  $l_4$  in  $D$ , such that  $a_{1,k_1} = a_{1,l_3}$  and  $a_{2,k_2} = a_{2,l_4}$ , we have that  $C_1 \cup \{l_4\}$  is not separated from  $C_2 \cup \{l_3\}$ . Otherwise, there only exists a column  $l'$  such that  $a_{1,k_1} = a_{1,l'}$ , and also have the column  $l$  such that  $a_{2,k_2} = a_{2,l'}$ .

Now, we remove two columns  $l$  and  $l'$  from  $D$ , then there are  $m - 1$  distinct elements in the first row of column set  $D \setminus \{l, l'\}$  and  $m - 1$  distinct elements in the second row of column set  $D \setminus \{l, l'\}$ . Since  $\frac{n-2(w-1)-2}{m-1} > m - 1$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D \setminus \{l, l'\}$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ . The proof is complete.  $\square$

## 4 A bound for $\text{SHF}(w_1 + w_2; n, m, \{w_1, w_2\})$

**Lemma 4.1** *Suppose  $A$  is a representation matrix of an  $\text{SHF}(2 + w; n, m, \{2, w\})$  with  $m \geq 2 + w$ . If there is a pair of elements  $x$  and  $y$  such that  $d_{ij}(x, y) \geq 2$ , then  $n < m^2 - m$ .*

*Proof:* Suppose that there exist an  $\text{SHF}(2 + w; m^2 - m, m, \{2, w\})$  with  $m \geq 2 + w$ , and its representation matrix contains a pair of elements  $a$  and  $b$  such that  $d_{ij}(x, y) \geq 2$ . By Lemma 2.1, we may assume  $d_{12}(a, b) \geq 2$ . Then we have the following table.

$$A = \begin{array}{|c|c|c|c|c|} \hline a & a & * & \cdots & * \\ \hline b & b & * & \cdots & * \\ \hline * & * & * & \cdots & * \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline * & * & * & \cdots & * \\ \hline \end{array}$$

Let  $\mathcal{C}$  denote the set of columns of  $A$ . We distinguish into the following 3 cases.

1. Suppose that there is at most one unique element in the first two columns of  $A$ .

By Lemma 2.1, we may assume the first columns and  $a_{2+w,2}$  are no unique element. Then there exist an column  $c_i$  of  $A$  such that  $a_{i1} = a_{ic_i}$  for  $2 < i \leq w+1$ . Let  $C_1 = \{2, c_i | 2 < i \leq w+1\}$ .

If there exist an column  $c_l$  such that  $a_{w+2,2} = a_{w+2,l}$  with  $c_l \notin C_1$ , then let  $C_2 = \{1, c_l\}$ , we have  $C_1$  is not separated from  $C_2$ ;

Otherwise, any column  $c_l$  satisfying  $a_{w+2,2} = a_{w+2,l}$ , we have  $c_l \in C_1$ . If  $|C_1| < w$ , then there exist two columns  $c_{l_1}$  and  $c_{l_2}$  satisfying  $a_{w+2,c_{l_1}} = a_{w+2,c_{l_2}}$  and  $\{c_{l_1}, c_{l_2}\} \cap C_1 = \emptyset$ . Let  $C_2 = \{1, c_{l_2}\}$ , we have  $C_1 \cup \{c_{l_1}\}$  is not separated from  $C_2$ ; If  $|C_1| = w$ , let  $\mathcal{C}_1 = \mathcal{C} - C_1$ . By the pigeon hole principle, there is an element  $t$  in row  $w+2$  such that  $\lambda_t^{w+2} \geq \lceil \frac{n-w}{m-1} \rceil = m$ . So we have  $d_{w+1,w+2}(z, t) \geq 2$  or  $d_{w+1,w+2}(a_{w+1,1}, t) \geq 1$  in  $\mathcal{C}_1$ . If  $d_{w+1,w+2}(z, t) \geq 2$ , then there exist two columns  $c_{l_1}$  and  $c_{l_2}$  in  $\mathcal{C}_1$  satisfying  $a_{w+1,c_{l_1}} = a_{w+1,c_{l_2}}$  and  $a_{w+2,c_{l_1}} = a_{w+2,c_{l_2}}$ . Let  $C_2 = \{1, c_{l_2}\}$ , we have  $C_1 \cup \{c_{l_1}\} \setminus \{c_{w+1}\}$  is not separated from  $C_2$ ; If  $d_{w+1,w+2}(a_{w+1,1}, t) \geq 1$ , then there exist two columns  $c_{l_1}$  and  $c_{l_2}$  in  $\mathcal{C}_1$  satisfying  $a_{w+1,c_{l_1}} = a_{w+1,1}$  and  $a_{w+2,c_{l_1}} = a_{w+2,c_{l_2}} = t$ . Let  $C_2 = \{1, c_{l_2}\}$ , we have  $C_1 \cup \{c_{l_1}\} \setminus \{c_{w+1}\}$  is not separated from  $C_2$ .

2. Suppose that there is two unique elements in the first two columns of  $A$ .

(i) The two unique elements in the same row. By Lemma 2.1, we may assume the last rows and first two columns are unique elements. Then there exist an column  $c_i$  of  $A$  such that  $a_{i1} = a_{ic_i}$  for  $2 < i \leq w$ . Let  $C_1 = \{2, c_i | 2 < i \leq w\}$ , and let  $\mathcal{C}_1 = \mathcal{C} - C_1$ . By the pigeon hole principle, there is an element  $t$  in row  $w+2$  such that  $\lambda_t^{w+2} \geq \lceil \frac{n-w}{m-2} \rceil = m+1$ . So we have  $d_{w+1,w+2}(z, t) \geq 2$  in  $\mathcal{C}_1$ . Then there exist two columns  $c_{l_1}$  and  $c_{l_2}$  in  $\mathcal{C}_1$  satisfying  $a_{w+1,c_{l_1}} = a_{w+1,c_{l_2}}$  and  $a_{w+2,c_{l_1}} = a_{w+2,c_{l_2}}$ . Let  $C_2 = \{1, c_{l_2}\}$ , we have  $C_1 \cup \{c_{l_1}\} \setminus \{c_{w+1}\}$  is not separated from  $C_2$ .

(ii) The two unique elements in the difference rows. By Lemma 2.1, we may assume the last two rows and first two columns contain unique elements. Then there exist an column  $c_i$  of  $A$  such that  $a_{i1} = a_{ic_i}$  for  $2 < i \leq w$ . Let  $C_1 = \{2, c_i | 2 < i \leq w\}$ , and let  $\mathcal{C}_1 = \mathcal{C} - C_1 \cup \{c_1\}$ . By the pigeon hole principle, there is an element  $t$  in row  $w+2$  such that  $\lambda_t^{w+2} \geq \lceil \frac{n-w}{m-1} \rceil = m$ . So we have  $d_{w+1,w+2}(z, t) \geq 2$  in  $\mathcal{C}_1$ . Then there exist two columns  $c_{l_1}$  and  $c_{l_2}$  in  $\mathcal{C}_1$  satisfying  $a_{w+1,c_{l_1}} = a_{w+1,c_{l_2}}$  and  $a_{w+2,c_{l_1}} = a_{w+2,c_{l_2}}$ . Let  $C_2 = \{1, c_{l_2}\}$ , we have  $C_1 \cup \{c_{l_1}\} \setminus \{c_{w+1}\}$  is not separated from  $C_2$ .

3. Suppose that there is at least three unique elements in the first two columns of  $A$ . By Lemma 2.1, we may assume the last  $k$  rows and first two columns contain unique elements,  $2 \leq k \leq w$ . Then there exist an column  $c_j$  of  $A$  such that  $a_{i1} = a_{ic_j}$  for  $2 < i \leq w+2-k$  and  $2 < j \leq w+2-k$ . Let  $C_1 = \{2, c_j | 2 < j \leq w+2-k\}$ , and let  $\mathcal{C}_1 = \mathcal{C} - C_1 \cup \{c_1\}$ .  $|C_1| \geq n+k-w-2 > (m-1)^2$ . By Lemma 1.3, we have two columns sets  $C_2$  and  $C_3$  with  $|C_2| = 1$  and  $|C_3| = k-1$  such that

$C_2$  and  $C_3$  are not separated in the last  $k$  rows. Thus, we have  $C_1 \cup \{C_3\}$  is not separated from  $C_2 \cup \{1\}$ . The proof is complete.  $\square$

**Theorem 4.2** *Suppose  $A$  is a representation matrix of an  $\text{SHF}(2+w; n, m, \{2, w\})$  with  $w \geq 2$  and  $m \geq 2+w$ , then  $n < m^2 - m + 3$ .*

*Proof:* We use induction on  $2+w$  to prove the theorem.

1. By Theorem 3.9, for  $w = 2$  this case satisfies.
2. Assume  $w > 2$  and there does not exist an  $\text{SHF}(w+1; m^2 - m + 3, m, \{2, w-1\})$ . Now, we need to prove that there does not exist an  $\text{SHF}(w+2; m^2 - m + 3, m, \{2, w\})$ .

Suppose that there is an  $\text{SHF}(w+2; m^2 - m + 3, m, \{2, w\})$ . Let  $A$  be a representation matrix of an  $\text{SHF}(w+2; m^2 - m + 3, m, \{2, w\})$ , and  $\mathcal{C}$  denote the set of columns of  $A$ . By removing the first row of  $A$ , we obtain a  $(w+1) \times (m^2 - m + 3)$  submatrix  $B$ . By inductive hypothesis, there are two sets of columns  $C_1$  and  $C_2$  in  $B$  with  $|C_1| = 2$  and  $|C_2| = w-1$  which are not separable. Now, we consider the same column sets  $C_1$  and  $C_2$  in  $A$ . Let  $\mathcal{C}_1 = \mathcal{C} - C_1$ . If  $C_1$  and  $C_2$  are not separable in the first row, then we have  $C_1$  and  $C_2$  are not separable in  $A$ , a contraction; If  $C_1$  and  $C_2$  are separable in the first row, then there exist two columns  $c_1$  and  $c_2$  satisfying  $c_1 \in \mathcal{C}_1$  and  $c_2 \in C_1$  such that  $a_{1,c_1} = a_{1,c_2}$ . Thus,  $C_1$  is not separated from  $C_2 \cup \{c_2\}$ , a contraction; Otherwise, there does not exist two columns  $c_1$  and  $c_2$  satisfying  $c_1 \in \mathcal{C}_1$  and  $c_2 \in C_1$  such that  $a_{1,c_1} = a_{1,c_2}$ . By the pigeon hole principle, there is an element  $t$  in the first row such that  $\lambda_t^1 \geq \lceil \frac{n-2}{m-1} \rceil = m+1$ . So we have  $d_{1,2}(t, z) \geq 2$  in  $\mathcal{C}_1$ . It is contradicting with Theorem 4.1.  $\square$

**Theorem 4.3** *If there exists an  $\text{SHF}(w_1+w_2; n, m, \{w_1, w_2\})$  with  $2 \leq w_1 \leq w_2$  and  $m \geq w_1 + w_2$ , then  $n < m^2 - m + 3$ .*

*Proof:* We use induction on  $w_1 + w_2$  to prove the theorem.

1. By Theorem 3.10, for  $w_1 = w_2$  this case satisfies.
2. By Theorem 4.2, for  $w_1 = 2$  and  $w_2 > w_1$  this case satisfies.
3. Assume  $w_1 > 2$  and  $w_2 > w_1$  and there does not exist an  $\text{SHF}(w_1+w_2-2; m^2 - m + 3, m, \{w_1-1, w_2-1\})$ . Now, we need to prove that there does not exist an  $\text{SHF}(w_1+w_2; m^2 - m + 3, m, \{w_1, w_2\})$ .

Suppose that there is an  $\text{SHF}(w_1 + w_2; m^2 - m + 3, m, \{w_1, w_2\})$ . Let  $A$  be a representation matrix of an  $\text{SHF}(w_1 + w_2; m^2 - m + 3, m, \{w_1, w_2\})$ , and  $\mathcal{C}$  denote the set of columns of  $A$ . By removing the first two rows of  $A$ , we obtain a  $(w_1 + w_2 - 2) \times (m^2 - m + 3)$  submatrix  $B$ . By inductive hypothesis, there are two sets of columns  $C_1$  and  $C_2$  in  $B$  with  $|C_1| = w_1 - 1$  and  $|C_2| = w_2 - 1$  which are not separable. Now, we consider the same column sets  $C_1$  and  $C_2$  in  $A$ . Let  $D = \mathcal{C} \setminus (C_1 \cup C_2)$ , then  $|D| \geq m^2 - 2m + 7$ . If  $C_1$  and  $C_2$  are not separable in the first two rows, then we have  $C_1$  and  $C_2$  are not separable in  $A$ , a contraction; If  $C_1$  and  $C_2$  are not separable in the first row or

the second row, then there exist two different columns  $c_1$  and  $c_2$  in  $D$  such that  $a_{2,c_1} = a_{2,c_2}$  or  $a_{1,c_1} = a_{1,c_2}$ . Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ , a contraction. Now, we consider the  $C_1$  and  $C_2$  are separable in the first two rows. Let  $X_i$  ( $i = 1, 2$ ) be the element set in which each element appears in the  $i$ -th row of these columns in  $D$ . Suppose that  $|X_1| \geq |X_2|$ . Now we distinguish into the following 4 cases.

(i)  $|X_1| \leq m - 2$ . Since  $\frac{n-w_1-w_2+2}{m-2} > m$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ .

(ii)  $|X_1| = |X_2| = m - 1$ . Since  $\frac{n-w_1-w_2+2}{m-1} > m - 1$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ .

(iii)  $|X_1| = m$  and  $|X_2| = m - 1$ . For any column  $k_i \in C_i$  ( $i = 1, 2$ ), we have  $a_{1,k_1} \in X_1$ ,  $a_{1,k_2} \in X_1$ , and  $\{a_{2,k_1}, a_{2,k_2}\} \cap X_2 \neq \emptyset$ . Without lose of generality, let  $a_{2,k_1} \in X_2$ . If there exist two columns  $l_1$  and  $l_2$  in  $D$ , such that  $a_{1,k_2} = a_{1,l_1}$  and  $a_{2,k_1} = a_{2,l_2}$ , we have that  $C_1 \cup \{l_2\}$  is not separated from  $C_2 \cup \{l_1\}$ ; Otherwise, there is a unique column  $l$  such that  $a_{1,k_2} = a_{1,l}$ , and  $a_{2,k_1} = a_{2,l}$ . We remove this column  $l$  from  $D$ , then there are  $m - 1$  distinct elements in the first row of column set  $D \setminus \{l\}$  and  $m - 2$  distinct elements in the second row of column set  $D \setminus \{l\}$ . Since  $\frac{n-n-w_1-w_2+1}{m-1} > m - 2$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D \setminus \{l\}$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ .

(iv)  $|X_1| = |X_2| = m$ . For any column  $k_i \in C_i$  ( $i = 1, 2$ ), we have  $a_{1,k_1} \in X_1$ ,  $a_{1,k_2} \in X_1$ ,  $a_{2,k_1} \in X_2$  and  $a_{2,k_2} \in X_2$ . If there exist distinct columns  $l_1$  and  $l_2$  in  $D$ , such that  $a_{1,k_2} = a_{1,l_1}$  and  $a_{2,k_1} = a_{2,l_2}$ , we have that  $C_1 \cup \{l_1\}$  is not separated from  $C_2 \cup \{l_2\}$ . Otherwise, there only exists a column  $l$  such that  $a_{1,k_2} = a_{1,l}$ , and  $a_{2,k_1} = a_{2,l}$ .

If there exist distinct columns  $l_3$  and  $l_4$  in  $D$ , such that  $a_{1,k_1} = a_{1,l_3}$  and  $a_{2,k_2} = a_{2,l_4}$ , we have that  $C_1 \cup \{l_4\}$  is not separated from  $C_2 \cup \{l_3\}$ . Otherwise, there only exists a column  $l'$  such that  $a_{1,k_1} = a_{1,l'}$ , and also have the column  $l$  such that  $a_{2,k_2} = a_{2,l'}$ .

Now, we remove two columns  $l$  and  $l'$  from  $D$ , then there are  $m - 1$  distinct elements in the first row of column set  $D \setminus \{l, l'\}$  and  $m - 1$  distinct elements in the second row of column set  $D \setminus \{l, l'\}$ . Since  $\frac{n-w_1-w_2}{m-1} > m - 1$ , by the pigeon hole principle, there exist two distinct columns  $c_1$  and  $c_2$  in  $D \setminus \{l, l'\}$  which agree in the first two rows. Thus,  $C_1 \cup \{c_1\}$  is not separated from  $C_2 \cup \{c_2\}$ . The proof is complete.  $\square$

## 5 A construction for SSHF with type $\{w_1, w_2\}$

In [35], the concept of strong separating hash families was introduced by Sarkar and Stinson, and they have a bound of it. We use the notation  $\text{SSHF}(N; n, m, \{w_1, w_2\})$  to denote a separating hash families with the type of  $\{1^q, w\}$  where  $w_1 = q, w_2 = w$  in this section.



**Lemma 5.1** *An  $SSH F(N; n, k+1, \{t, w\})$  is equivalent to an  $SH F(N; n, k+1, \{1^t, w\})$ .*

For  $2 < l < k < n$  let  $M(n, k, l)$ , the covering number, denote the minimal size of a family  $\mathcal{K}$ , of  $k$ -element subsets of  $\{1, 2, \dots, n\}$  having the property that every  $l$  element set is contained in at least one  $K \in \mathcal{K}$ .

**Theorem 5.2** ([28]) *For positive integers  $k, l$ ,*

$$M(n, k, l) \leq (1 + o(l)) \frac{\binom{n}{l}}{\binom{k}{l}},$$

where the  $o(l)$  term tends to zero as  $n$  tends to infinity.

Now, we will use a covering to construct the  $SSH F(N; n, m, \{w_1, w_2\})$ . There are some simple definitions and properties about *hypergraph*. A hypergraph is a pair  $H = (V, E)$ , where  $V$  is a finite set whose elements are called vertices and  $E$  is a family of subsets of  $V$ , called edges. It is  $k$ -uniform if each of its edges contains precisely  $k$  vertices. Let  $M(n, k, l)$  denote the minimum possible number of edges of an  $k$ -uniform hypergraph that any  $l$  vertices is contained in at least one edge.

Let  $H = (V, E)$  be an  $k$ -uniform hypergraph that any  $l$  vertices is contained in at least one edge, where  $V = \{x_1, x_2, \dots, x_n\}$  and  $E = \{B_1, B_2, \dots, B_N\}$ . Now, let  $B_i = \{x_{i,1}, x_{i,2}, \dots, x_{i,k}\}, 1 \leq i \leq N$ . we constructed an  $N \times n$  matrix  $A = (a_{i,j})$  by:

$$a_{i,j} = \begin{cases} l, & \text{if } x_j \in B_i \text{ and } x_j = x_{i,l}; \\ 0, & \text{otherwise.} \end{cases}$$

By the rule of above, we can obtain an  $N \times n$  matrix  $A = (a_{i,j})$ .

**Lemma 5.3** *If there exists an  $k$ -uniform hypergraph that any  $t$  vertices is contained in at least one edge, then there exists an  $SSH F(N; n, t+1, \{t, w\})$  with  $N \leq \frac{C_n^t}{C_k^t} (1 + o(t))$ , where the  $o(t)$  term tends to zero as  $n$  tends to infinity.*

*Proof:* Let  $V = \{x_1, x_2, \dots, x_n\}$  and  $E = \{B_1, B_2, \dots, B_N\}$ . Now, we obtained a matrix  $A$  by the construction of above. In the following, we will show that  $A$  is a representation matrix of  $SSH F(N; n, k+1, \{t, w\})$ . From Lemma 5.1, we only to show that  $A$  is a representation matrix of  $SH F(N; n, k+1, \{1^t, w\})$ . Let  $C_1, C_2, \dots, C_{t+1}$  be disjoint the columns sets of  $A$  with  $|C_{t+1}| = w$  and  $|C_i| = 1$  for  $i = 1, 2, \dots, t$ . From the the  $k$ -uniform hypergraph that any  $t$  vertices is contained in at least one edge, we can known every set with  $t$  distinct vertices is contained in at least one edge, so there exist a positive integer  $j$  such that  $C_1 \cup C_2 \cup \dots \cup C_t \subset B_j$ . So by the construction, we obtained  $j$ th row of  $A$  such that any element in  $C_1 \cup C_2 \cup \dots \cup C_t$  is a unique element. Thus  $C_1, C_2, \dots, C_{t+1}$  is separated by the row  $j$ .  $\square$

## 6 Conclusion

In this paper we mainly investigate the bounds of separating hash families. Firstly, by the some small parameter, we construct some submatrixs which are forbidden configuration. Thus, We get the optimal  $\text{SHF}(4; 10, 4, \{2, 2\})$  and improve the bound of  $\text{SHF}(4; n, m, \{2, 2\})$  and  $\text{SHF}(2 + w; n, m, \{2, w\})$ . By the induction hypothesis, we improve the bound of  $\text{SHF}(2w; n, m, \{w, w\})$  and  $\text{SHF}(w_1 + w_2; n, m, \{w_1, w_2\})$ . Secondly, we use the  $k$ -uniform hypergraph to construct the SSHF with type  $\{w_1, w_2\}$ .

## References

- [1] N. Alon, G. Cohen, M. Krivelevich, S. Litsyn, Generalized hashing and parent-identifying codes. *J. Combin. Theory Ser. A* **104**(1) (2003), 207-215.
- [2] N. Alon, R. A. Duke, H. Lefmann, V. Rödl, R. Yuster, The algorithmic aspects of the regularity lemma. *J. Algorithms* **16**(1) (1994), 80-109.
- [3] N. Alon, E. Fischer, M. Szegedy, Parent-identifying codes. *J. Combin. Theory Ser. A* **95**(2) (2001), 349-359.
- [4] N. Alon, U. Stav, New bounds on parent-identifying codes: the case of multiple parents. *Combin. Probab. Comput.* **13**(6) (2004), 795-807.
- [5] M. Atici, S. S. Magliveras, D. R. Stinson, W. D. Wei, Some recursive constructions for perfect hash families. *J. Comb. Des.* **4** (1996), 353-363.
- [6] M. Bazrafshan, T. Trung, Bounds for separating hash families. *J. Combin. Theory Ser. A* **118** (2011), 1129-1135.
- [7] M. Bazrafshan, T. Trung, Improved bounds for separating hash families. *Des. Codes Cryptogr.* **69** (2013), 369-382.
- [8] M. Bazrafshan, Separating hash families. PhD thesis, University of Duisburg-Essen (2011).
- [9] S. R. Blackburn. Perfect hash families: probabilistic methods and explicit constructions. *J. Combin. Theory Ser. A* **92**(1) (2000), 54-60.
- [10] S. R. Blackburn, An upper bound on the size of a code with the  $k$ -identifiable parent property. *J. Combin. Theory Ser. A* **102**(1) (2003), 179-185.
- [11] S. R. Blackburn, Perfect hash families with few functions. Unpublished manuscript, 2000; available online as IACR research report 2003/17; see <http://eprint.iacr.org/2003/017>
- [12] S. R. Blackburn, Frameproof codes. *SIAMJ. Discret. Math.* **16**(3) (2003), 499-510.
- [13] S. R. Blackburn, T. Etzion, D. R. Stinson, G. M. Zaverucha, A bounds on the size of separating hash families. *J. Combin. Theory Ser. A* **115** (2008), 1246-1256.
- [14] D. Boneh, J. Shaw, Collusion-free fingerprinting for digital data. *IEEE Trans. Inform. Theory.* **44** (1998), 1897-1905.
- [15] C. J. Colbourn, J. H. Dinitz, Handbook of Combinatorial Designs, 2nd Ed Chapman & Hall/CRC,(2007).
- [16] M. Cheng, L. Ji, Y. Miao Separable codes. *IEEE Trans. Inf. Theory.* **58** (2012), 1791-1803.
- [17] M. Cheng, Y. Miao, On anti-collusion codes and detection algorithms for multimedia fingerprinting. *IEEE Trans. Inf. Theory.* **57** (2011), 4843-4851.

- [18] M. L. Fredman, J. Komlos, On the size of separating systems and families of perfect hash functions. *SIAM J. Algebraic Discret. Methods* **5** (1984), 61-68.
- [19] R. Fuji-Hara, Perfect hash families of strength three with three rows from varieties on finite projective geometries. *Des. Codes Cryptogr.* **77**(2015), 351-356.
- [20] F. Gao, G. Ge, New Bounds on Separable Codes for Multimedia Fingerprinting. *IEEE Trans. Inf. Theory.* **60** (2014), 5257-5262.
- [21] G. Ge, C. Shangguan, Separating hash families: A Johnson-type bound and new constructions. <http://arXiv:1601.04807v1>, 2016.
- [22] C. Guo, D. R. Stinson, T. Trung, On tight bounds for binary frameproof codes. *Des. Codes Cryptogr.* **77** (2015), 301-319.
- [23] C. Guo, D. R. Stinson, A tight bound on the size of certain separating hash families. <http://arXiv:1510.00293v1>, 2015.
- [24] H. D. L. Hollmann, J. H. van Lint, J. P. Linnartz, L. M. G. M. Tolhuizen, On codes with the identifiable parent property. *J. Combin. Theory Ser. A* **82**(2) (1998), 121-133.
- [25] P. C. Li, R. Wei, G. H. J. van Rees, Constructions of 2-cover-free families and related separating hash families. *J. Combin. Designs* **14**(2006), 423-440.
- [26] S. Martirosyan, T. Trung, Explicit constructions for perfect hash families. *Des. Codes Cryptogr.* **46**(1) (2008), 97-112.
- [27] A. Procacci, R. Sanchis, Perfect and separating Hash families: new bounds via the algorithmic cluster expansion local lemma. <http://arXiv:1601.0538v1>, 2016.
- [28] V. Rödl, On a packing and covering problem, *Eur. J. Combinatorios.* **6**(1) (1985), 69-78.
- [29] C. Shangguan, X. Wang, G. Ge, Y. Miao, New bounds for frameproof codes <http://arXiv:1411.5782v1>, 2014.
- [30] J. N. Staddon, D. R. Stinson, R. Wei, Combinatorial properties of frameproof and traceability codes. *IEEE Trans. Inform. Theory.* **47** (2001), 1042-1049.
- [31] D. R. Stinson, R. Wei, Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM J. Discrete Math* **11**(1)(1998), 41-53.
- [32] D. R. Stinson, T. Trung, R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *J. Statist. Plan. Inference.* **86** (2000), 595-617.
- [33] D. R. Stinson, R. Wei, K. Chen, On generalized separating hash families. *J. Combin. Theory Ser. A* **115** (2008), 105-120.
- [34] D. R. Stinson, G. M. Zaverucha, Some improved bounds for secure frameproof codes and separating hash families. *IEEE Trans. Inf. Theory.* **54**(2008), 2508-2514.
- [35] P. Sarkar, D. R. Stinson, Frameproof and IPP codes. *Lecture Notes in Computer Science.* **2247** (2001), 117-126.
- [36] T. Trung, A tight bound for frameproof codes viewed in terms of separating hash families. *Des. Codes Cryptogr.* **72**(2014), 713-718.
- [37] R. A. Walker II, C. J. Colbourn, Perfect hash families: constructions and existence. *J. Math. Cryptol.* **1**(2), (2007), 125-150.